McAfee Research Report

McAfee

June 2009 Spam Report

McAfee Avert Labs Discovers and Discusses Key Spam Trends

Key Findings

President Obama's First 100 Days of Spam

Although you might imagine the change of administration in the United States would have a major impact on the Internet, the first 100 days of Obama's presidency were mostly business as usual in the spam world.

Identifying Spam Trends of the Future

Even though we've been told to avoid clicking such links to prevent spammers from learning who we are, many of us forget to be vigilant because the overall detection accuracy of anti-spam products has improved.

Recipients may instantly distrust an executable attached to an email, but they often feel unthreatened by a short blurb and a URL.

Table of Contents

President Obama's First 100 Days of Spam

As President Barack Obama was celebrating his election victory, the spamming community was dealt a heavy blow. One of the major low-cost hosting facilities that was heavily used by spammers and malware authors to host their websites and centralize their command and control systems was forced to close. As a direct result, global spam volumes collapsed from constant announcements of "all-time record highs" to unexciting 2007-level lows. Was this a sign of things to come? Could this be the end of the spam industry as we know it?

But the spammers weren't down for long. Spam volumes were recovering even before President Obama took office, as a steady linear increase in volume preceded the inauguration. A number of new employment and Internet money scams hound a worldwide economy wracked by fear and paranoia. Here's a lighthearted look at spam activity during the first 100 days of the new administration.

Days 1-30

After the inauguration, volumes headed downhill, with Obama-related spam falling exponentially after the election. The discussion on the Democrats stimulus package marked the beginning of a steady downturn in spam volume. The bill passed the House of Representatives one week later, on January 29.

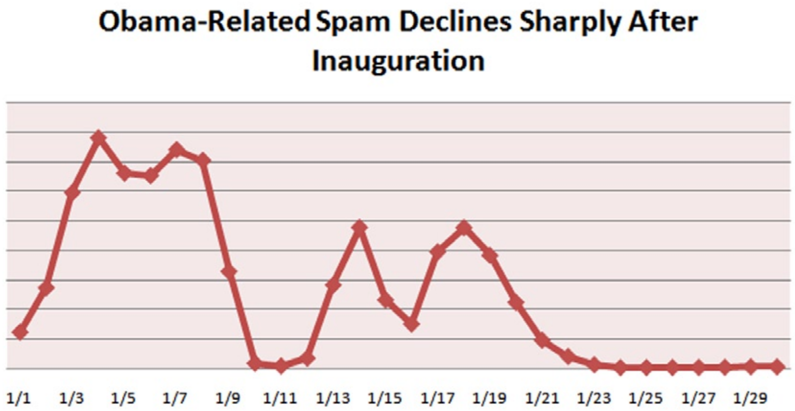


Figure 1: We weren't surprised to see spam related to President Obama drop off rapidly after he took office.

In the first two weeks of February everyone was scurrying around: Security researchers were looking for any indications of a Valentine's Day spam surprise, and the new administration's computer geeks complained about having to use a hardened version of Microsoft Windows in the White House instead of their Macintoshes.

With the capping of executive reimbursement plans for companies receiving funds from the Fed's Troubled Asset Relief Program , we saw some related Valentine e-card spam leading up to the big day, but the email was mostly generic pharmacy or replica-watch spam with a different catch phrase. The big burst of Valentine's Day e-card spam came just afterward, when Secretary of State Hillary Clinton began her trip to Asia. That time was also when the Torpig botnet owners managed to regain control of their network from the University of California, Santa Barbara researchers who had managed to hijack it for 10 days.

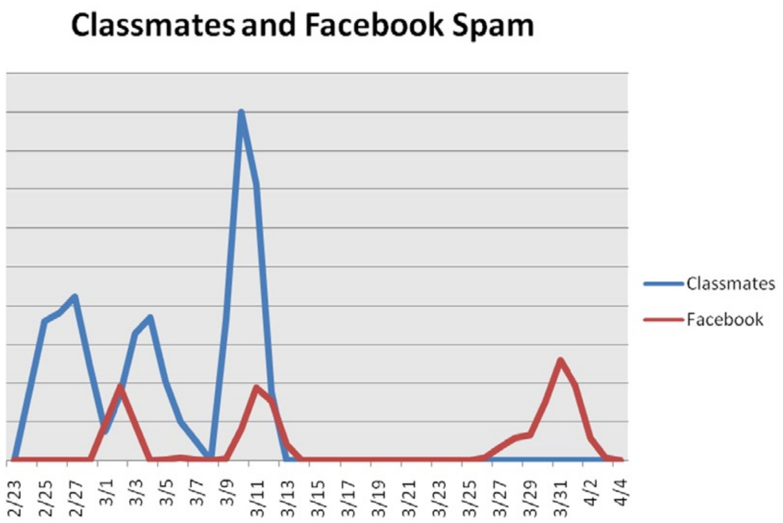


Figure 2: In February a new spam campaign, based on an appeal to school "classmates," enjoyed a brief surge.

Days 31-60

With traffic volumes continuing to decline, replica watches dominated emails until a new breed of "classmates" spam popped up during the last week of February. The school connection remained strong into the first week of March, when British Prime Minister Gordon Brown visited President Obama. Classmates spam tag-teamed with Facebook spam by the second week in March as the Omnibus Appropriations bill was pushed through Congress and a White House Council on Women and Girls was convened. With Obama's stimulus package through the U.S. Senate and waiting on his desk, the third week in March saw pharmaceutical spam lead the field. Drugs maintained first place even as Obama held meetings with a series of global policy makers, including the president of Brazil, the prime ministers of Australia and Ireland, ex-Soviet Premier Mikhail Gorbachev, and even "Tonight Show" host Jay Leno. While normally March is a big month for spam, the final results were down this year. Steadily declining traffic volumes indicated that there had been a few hitches in delivering the usual spam barrage.

As April approached, everyone started to hear about Conficker, the zombie botnet that had been seeding itself on e-cards, Valentines, and UPS invoices. Conficker was never going to send spam and malware, but rumors sprang up about its dealing a devastating April Fool's joke on all of its infected hosts. As Vice President Joseph Biden went to Chile, President Obama announced a new strategy for Afghanistan. With a focus on April 1 and not knowing what Conficker would do (combined with a number of wild assumptions of worst-case scenarios), we hoped Obama would sweep in with a sack of government money to make the problem go away.

Days 61-100

With the April 1 deadline for network insanity looming, President Obama rushed off to an emergency meeting of the G20 leaders to discuss the economic implications of worldwide financial disaster. Conficker predictions turned out to be a Y2K-like exaggeration: April 1 came and went without any world-changing botnet attack or big infusion of government money.

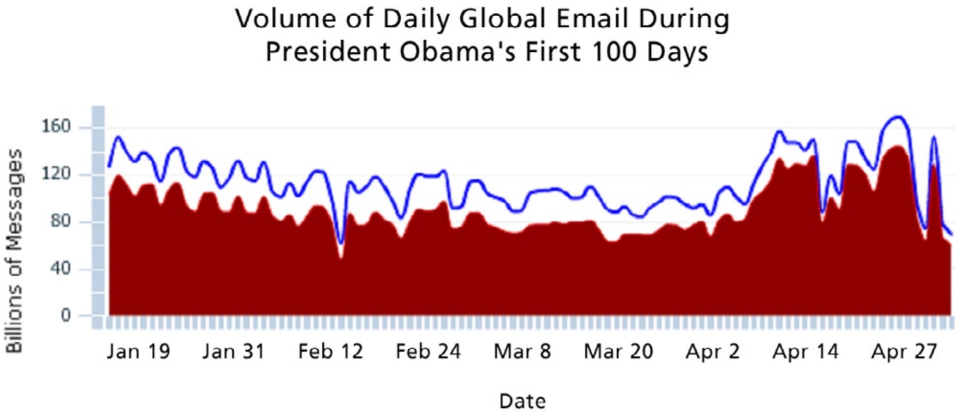


Figure 3: Spam email traffic, shown in red, rose rapidly in early April. The blue line represents all messages. The gap between the two lines is legitimate email.

Between April 1 and April 8, global spam volumes nearly doubled, moving from a three-month low to a four-month high. Obama met with NATO leaders as well as the Alliance of Civilizations forum to discuss the global interconnectedness of our 21st-century world. With spam volumes increasing exponentially, the president made a detour to visit the troops in Iraq.

Swimming in the high tide of spam, the second week in April was fraught with danger as an American freighter captain was taken hostage by Somali pirates and the deadline to pay taxes loomed. Faced with tax scams and an abundance of enhancement spams, President Obama gave the approval to use force to free the trapped captain.

On April 13, Obama allowed Americans with Cuban heritage to travel and send money to their relatives. Spammers responded with an anti-viral and anti-bacterial spam campaign that ended up selling the same old elixir of carnality as always.

A few controversial memos on the nature of torture and the legality of interrogations were released by the White House in the third week of April. Spammers immediately responded with open arms and greetings of "Wazzup?" "Hi there," "Hello," "Good morning," and "good evening" in the subjects of their mails. Though our email boxes looked friendlier at first, spammers had not actually changed their tune. They were simply masking the familiar genital-maintenance routine with a new presentation. Within a week that new face had fallen away to subject lines of massive "77%-off discounts."

President Obama spoke at a Holocaust remembrance ceremony on April 23, which coincided with a number of virus-laden "WorldPay Card" emails and an increase in phishing emails. Payment information, account updates, and rumors of canceled registrations filled the Internet with their identity-stealing methods through Obama's 100th day, on April 29.

Conclusion

Although you might have imagined the change of administration in the United States would have a major impact on the Internet, we've seen that the first 100 days of Obama's presidency were mostly business as usual in the spam world. Spammers continued to traffic in cut-rate watches, phony pharmaceuticals, hoary hoaxes, and identity theft. Even the big setback of the loss of a major hosting center slowed the spam tide only temporarily.

President Obama's administration is the first one in U.S. history that will have to seriously tackle the issues created by an interconnected world. It will be interesting to follow his proposed policies to see if they have any more impact than those of previous governments.

Identifying Spam Trends of the Future

We have seen an increase in spam that either uses the look and feel of a social networking site, or includes "unsubscribe" links that serve the same purpose as clicking the main link. This trend, which has been tried before, creates legitimate-looking spam by incorporating familiar features into the emails. Even though we've been told to avoid clicking such links to prevent spammers from learning who we are, many of us forget to be vigilant because the overall detection accuracy of anti-spam products has improved. This carelessness can result in a higher click rate on the fewer spam messages that do bypass the filters. We expect this unfortunate trend will continue.

Why is this trend likely to continue? The nature of spam relies largely on the whims of the bot masters; conceptually they can do almost anything that a computer can do. So almost anything is possible.

Spam campaign effectiveness is a function of three elements:

- Messages sent
- Spam catch rate
- Hits per email delivered

Messages sent is a function of three further elements:

- Botnet size
- Message size
- Email list size

The most important qualities of an email campaign combine these elements:

- Botnet size
- Message size
- Email list size
- Spam catch rate
- Hits per email delivered

Of these top qualities, botnet size is something that doesn't come into play when determining trends. A bigger botnet sends more mail, so it may be easier to notice; but just because there is a lot of mail today doesn't mean that the campaign will continue.

Email list size is also relatively difficult to measure. Bot masters will use their Trojan-infected zombie computers to gather any email addresses that the victim has in the address book. Bots will continue to add to their list of email addresses in that manner.

Spammers might want to increase the message size to decrease the spam catch rate or increase the hits per email delivered, but they are held back by the need to keep their messages small. The smaller a message is, the faster a zombie host can generate and send it.

A few years ago, numerous anti-spam products had significant problems trying to detect the "spamness" of images in pump-and-dump stock emails. Even after the novelty wore off, we continued to see a steady stream of "the world is drowning in image spam" articles and news reports.

When no product could effectively stop image spam, network administrators had a much lower spam catch rate, which meant that more of those emails were getting into individual email inboxes. Further, spammers wanted victims to go to their own stock market trading accounts; thus no URL was necessary and there was no significance to measuring hits per email delivered.

Now let's take a look at three email features that have been inherited from successful phishing and spam campaigns: branding, images, and headline spam.

Branding

The first of these is branding. Successful phishing campaigns work because they look just like the real thing, such as a bank's email. A victim may click the link in the email without thinking twice about it. This same technique can be applied to both malware and everyday spam. In late February and early March we noticed a number of emails spoofing Classmates and Facebook that followed up on an actual Classmates.com marketing campaign. The false messages attempted to get the recipient to click a link and download a "Flash Player installer," which was really malware.

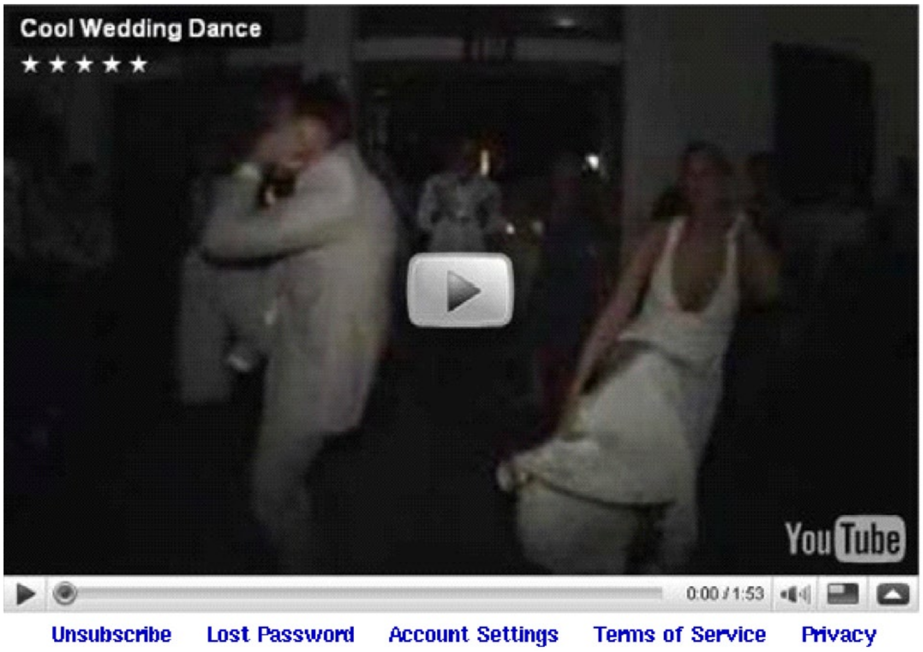
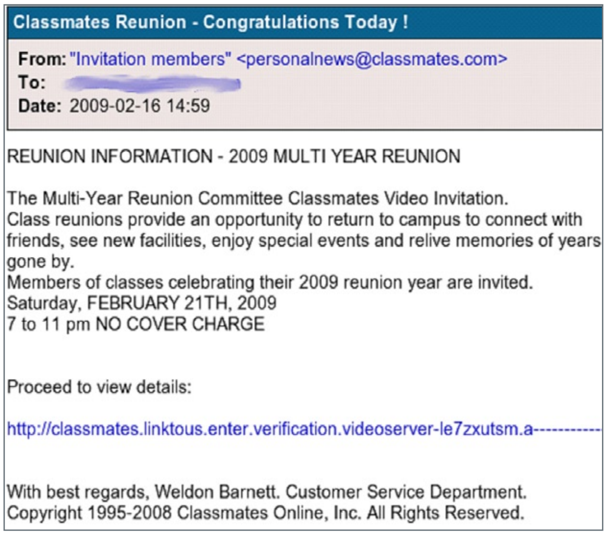


Figure 4: Example of Classmates video spam.



Classmates Reunion - Congratulations Today !

From: "Invitation members" <personalnews@classmates.com>
To: [redacted]
Date: 2009-02-16 14:59

REUNION INFORMATION - 2009 MULTI YEAR REUNION

The Multi-Year Reunion Committee Classmates Video Invitation.
Class reunions provide an opportunity to return to campus to connect with friends, see new facilities, enjoy special events and relive memories of years gone by.
Members of classes celebrating their 2009 reunion year are invited.
Saturday, FEBRUARY 21TH, 2009
7 to 11 pm NO COVER CHARGE

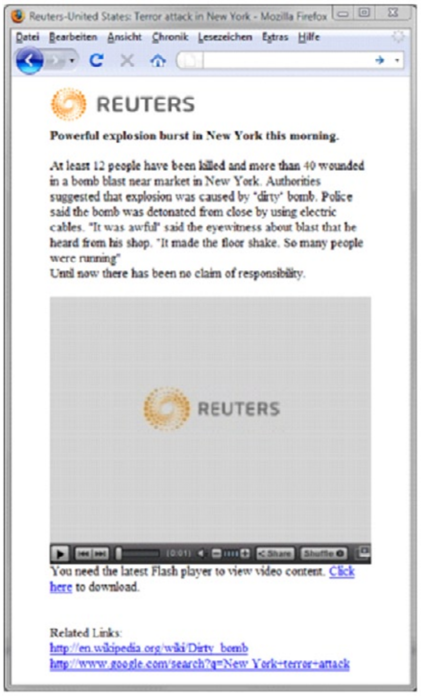
Proceed to view details:

http://classmates.linktous.enter.verification.videoserver-le7zxutsm.a----------

With best regards, Weldon Barnett. Customer Service Department.
Copyright 1995-2008 Classmates Online, Inc. All Rights Reserved.

Figure 5: Example of Classmates spam.

In March, we saw the same branding in headline spam associated with fictional bomb attacks, with websites trying to look like legitimate video feeds from Reuters news service.


Reuters-United States: Terror attack in New York - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
REUTERS

Powerful explosion burst in New York this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in New York. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was detonated from close by using electric cables. "It was awful" said the eyewitness about blast that he heard from his shop. "It made the floor shake. So many people were running"
Until now there has been no claim of responsibility.

You need the latest Flash player to view video content. Click here to download.

Related Links:
http://en.wikipedia.org/wiki/Dirty_bomb
http://www.google.com/search?q=New York+terror+attack

Figure 6: Example of branding spam.

Branding can be very cheap because a spammer can reference external images instead of placing them all in an email. Thus the message size does not increase, but the hits per email delivered does rise. That makes this a winning strategy for spammers, and one that we're likely to see more of.

Images

Another popular attack is image spam associated with enlargement drugs. In these emails we find an attached image and a reference to a Chinese website for purchasing pharmaceuticals. Applying these same points to our analysis, we see the message size increasing, which makes the campaign roll out more slowly. Using images with URLs written into them may be harder to identify, which reduces the spam catch rate, but this method is also unlikely to get a lot of people to bite, because they have to manually enter the website into their browsers, which reduces the spam's effectiveness. This is not a strong spam strategy. A number of anti-spam products are equipped with image-spam detection engines, so the spam catch rate is likely to remain high and discourage spammers from using this method.

Headline Spam

Many of us love to read the news and feel well-informed, and across the Internet news (accurate or not) spreads like wildfire through short emails, instant messages, and tweets. Headline spam has been recycling yesterday's news for a long time, and it is certain to continue.

A subject line or short message blurb "Check out this video of something" and a link is all that an email needs to lure people into clicking to see something new. This email is very cheap to produce, which gives it a very small message size, and they can be sent in huge batches. It is reasonable to imagine that the hits-per-email-delivered mark is relatively high in this case, because the lure of news combined with bored users (at work or elsewhere) can easily produce a hit even though the recipient knows that the email may be bogus. Recipients may instantly distrust an executable attached to an email, but they often feel unthreatened by a short blurb and a URL.

Add to that the competition of 24-hour news and you have a self-perpetuating cycle, in which something happens to produce a news story, headline spam appears that fuels the fire and results in the news story appearing to have more relevance than before, and the headline spam continues into another round.

Swine Flu

The swine flu panic is a perfect example of headline spam. The first flu-related spam that referenced swine flu weren't trying to sell Tamiflu (though some claimed to be); they were generic Canadian pharmacy websites trying to sell genital maintenance pills.

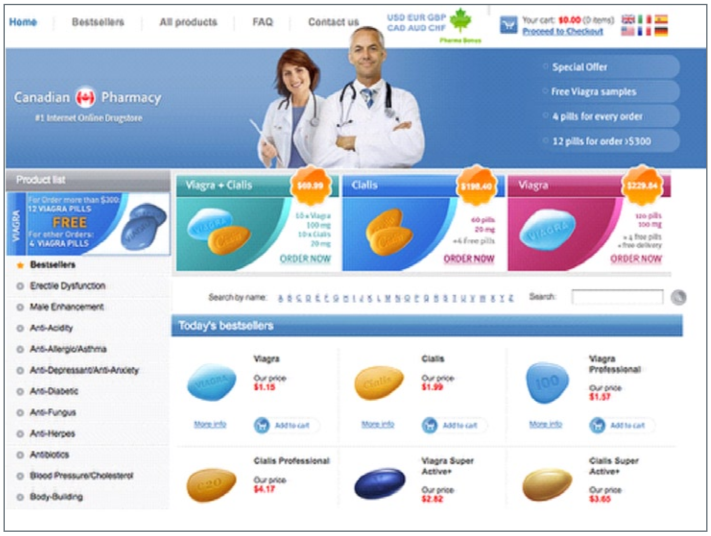
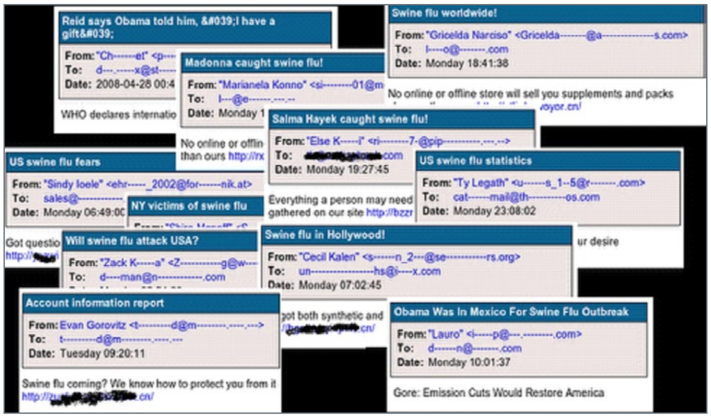


Figure 7: Example of swine flu website.



Reid says Obama told him, &#039;I have a gift&#039;

From: "Ch------el" <p---
To: d---.-----x@st-----
Date: 2008-04-28 00:4

WHO declares internatio

Swine flu worldwide!

From: "Gricelda Narciso" <Gricelda-------@a-------------s.com>
To: l----o@-------.com
Date: Monday 18:41:38

No online or offline store will sell you supplements and packs
voyor.cn/

Madonna caught swine flu!

From: "Marianela Konno" <si--------01@m
To: l---@e------.---.--
Date: Monday 1

No online or offlin
than ours http://rx

Salma Hayek caught swine flu!

From: "Else K-----i" <ri--------7-@pip----------.---.-->
To: [redacted].com
Date: Monday 19:27:45

Everything a person may need
gathered on our site http://bzzr

US swine flu fears

From: "Sindy Ioele" <ehr-----_2002@for------nik.at>
To: sales@-----------
Date: Monday 06:49:00

US swine flu statistics

From: "Ty Legath" <u------s_1--5@r-------.com>
To: cat------mail@th----------os.com
Date: Monday 23:08:02

ur desire

NY victims of swine flu

Got questio
http://[redacted]

Will swine flu attack USA?

From: "Zack K-----a" <Z-----------g@w---
To: d----man@n-----------.com

Swine flu in Hollywood!

From: "Cecil Kalen" <s------n_2---@se-----------rs.org>
To: un----------------hs@i----x.com
Date: Monday 07:02:45

got both synthetic and
//[redacted].cn/

Account information report

From: Evan Gorovitz <t---------d@m--------.----.--->
To: t---------d@m--------.----.---
Date: Tuesday 09:20:11

Swine flu coming? We know how to protect you from it
http://zu[redacted].cn/

Obama Was In Mexico For Swine Flu Outbreak

From: "Lauro" <i-----p@---.--------.com>
To: d------n@-------.com
Date: Monday 10:01:37

Gore: Emission Cuts Would Restore America

Figure 8: Examples of swine flu spam email headers.

This spam was generated a few days after the initial, legitimate news headlines appeared. The World Health Organization announced that the swine flu was a public health emergency on April 25, and incremented the pandemic alert to level 4 on April 27.

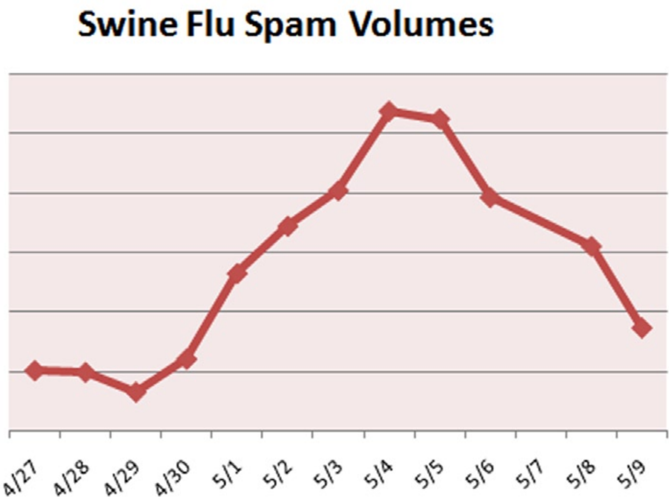


Figure 9: Spam referencing swine flu peaked about a week after the emergency was named a pandemic.

The first round of swine flu spam was purely a reaction by the spammers to something that was in the news. Pharmacy spam was already the biggest occurrence of the headline spam theme. The fact that they actually sold pharmaceuticals and that the flu-related stories could be easily related to pharmaceuticals was almost coincidental.

Because the story continued to gain interest in the international media, so did the headline spam associated with it. As the course of the story has moved from worldwide pandemic during the first week toward an overreaction, swine flu spam traffic has predictably started to decline.

Conclusion

What does the future of spam hold for us? Spam is all about making money and, as with most businesses, spammer CEOs need to worry about costs and their bottom lines. As long we continue to behave as suckers, spammers will use sophisticated tactics to separate us from our money.

Brought to You by McAfee Avert Labs

McAfee Avert Labs is the global research group of McAfee, Inc. With research teams devoted to malware, potentially unwanted programs, host intrusions, network intrusions, mobile malware, and ethical vulnerability disclosure, Avert Labs enjoys a broad view of security. This expansive vision allows McAfee's researchers to continually improve security technologies and better protect the public.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com